

CLAIMS

1. A parallelizable integrity-aware encryption method, the method comprising the steps of:
whitening at least one message block with a first mask
5 value;
encrypting the whitened at least one message block
using a block cipher and a first key; and
whitening the encrypted at least one message block with
a second mask value to generate at least one corresponding
10 output ciphertext block.
2. The method of claim 1, wherein the first and second
mask values are computed by applying a XOR function to a
first value derived from a NONCE value and a second value
derived from encrypting a third value using the block cipher
15 and a second key, and then applying a substitution function
to the result of the XOR function.
3. The method of claim 2, wherein the first value derived
form the NONCE value is computed by encrypting the NONCE
value using the block cipher and the first key.
- 20 4. The method of claim 2, wherein the third value is a
unique counter value or random number.
5. The method of claim 2, wherein the steps of whitening
each comprise the step of applying a XOR function, the first
and second mask values being equal.
- 25 6. The method of claim 1, further comprising the steps of:
applying a XOR function to all message blocks of a
message to compute a XOR-sum;
applying a third mask value to the XOR-sum;
encrypting the masked XOR-sum using the block cipher
30 and the first key; and

applying a fourth mask value to the encrypted XOR-sum
to generate an integrity tag.

7. The method of claim 6, wherein the third and fourth
mask values are computed by applying a XOR function to a
5 first value derived from a NONCE value and a second value
derived from encrypting a third value using the block cipher
and a second key, and then applying a substitution function
to the result of the XOR function.
8. The method of claim 1, further comprising the steps of:
10 whitening the at least one output ciphertext block with
the second mask value;
decrypting the at least one whitened ciphertext block
using a block cipher and a first key; and
whitening the at least one decrypted block with a first
15 mask value to generate at least one corresponding message
block.
9. The method of claim 1, wherein the block cipher is
selected from the group consisting of: an Advanced
Encryption Standard (AES) block cipher, a Data Encryption
20 Standard (DES) block cipher, and a Triple Data Encryption
Standard (3DES) block cipher.
10. At least one signal embodied in at least one carrier
wave for transmitting a computer program of instructions
configured to be readable by at least one processor for
25 instructing the at least one processor to execute a computer
process for performing the method as recited in claim 1.
11. At least one processor readable carrier for storing a
computer program of instructions configured to be readable
by at least one processor for instructing the at least one
30 processor to execute a computer process for performing the

method as recited in claim 1.

12. A parallelizable integrity-aware encryption method, the method comprising the steps of:

applying a XOR function to all blocks of a message to
5 compute a XOR-sum;
applying a first mask value to the XOR-sum;
encrypting the masked XOR-sum using a block cipher and
a first key; and
applying a second mask value to the encrypted XOR-sum
10 to generate an integrity tag.

13. The method of claim 12, wherein the first and second mask values are computed by applying a XOR function to a first value derived from a NONCE value and a second value derived from encrypting a third value using the block cipher
15 and a second key, and then applying a substitution function to the result of the XOR function.

14. The method of claim 13, wherein the first value derived from the NONCE value is computed by encrypting the NONCE value using the block cipher and the first key.

20 15. The method of claim 12, further comprising the steps of:

whitening at least one message block with a third mask value;
encrypting the whitened at least one message block
25 using the block cipher and the first key; and
whitening the encrypted at least one message block with the third mask value to generate a corresponding output ciphertext block.

16. The method of claim 15, wherein the steps of whitening
30 each comprise the step of applying a XOR function.

17. The method of claim 15, wherein the third mask value is computed by applying a XOR function to a first value derived from a NONCE value and a second value derived from encrypting a third value using the block cipher and a second key, and then applying a substitution function to the result of the XOR function.

18. The method of claim 12, wherein the block cipher is selected from the group consisting of: an Advanced Encryption Standard (AES) block cipher, a Data Encryption Standard (DES) block cipher, and a Triple Data Encryption Standard (3DES) block cipher.

19. At least one signal embodied in at least one carrier wave for transmitting a computer program of instructions configured to be readable by at least one processor for instructing the at least one processor to execute a computer process for performing the method as recited in claim 12.

20. At least one processor readable carrier for storing a computer program of instructions configured to be readable by at least one processor for instructing the at least one processor to execute a computer process for performing the method as recited in claim 12.